06-30-00 A

FORM PTO-1082

Box Patent Application
ASSISTANT COMMISSIONER FOR PATENTS
Washington D.C., 20231

Case Docket No.: 81674-265754
Date: June 29, 2000
Express Mail Label No.: EL 594 170 469 US

Dear Sir:

Transmitted herewith for filing is the patent application of
Inventor(s): Ernie F. BRICKELL of Portland, Oregon
For: SYSTEM AND METHOD FOR CREATION AND USE OF STRONG PASSWORDS

Enclosed are:

X 7 Sheets of formal drawings
X An assignment of the invention to Intel Corporation.
X Declaration and Power of Attorney.

CALCULATION OF FEES

| | ITEM | NO. OF CLAIMS FILED MINUS BASE* | NO. OF CLAIMS OVER BASE | X SM/LG ENTITY FEE | $ AMOUNT | FEE |
|---|---|---|---|---|---|---|
| A | TOTAL CLAIMS FEE | 34 -20*= | 14 | x $9 or x $18 | $ 252 | |
| B | INDEPENDENT CLAIMS FEE** | 6 - 3*= | 3 | x$39 or x 78 | $234 | |
| C | SUBTOTAL – ADDITIONAL CLAIMS FEE (ADD FINAL COLUMN IN LINES A + B) | | | | | $486 |
| D | MULTIPLE-DEPENDENT CLAIMS FEE | | | SMALL ENTITY FEE = $130 LARGE ENTITY FEE = $260 | | $0 |
| E | BASIC FEE* | | | SMALL ENTITY FEE = $345 LARGE ENTITY FEE = $690 | | $690 |
| F | TOTAL FILING FEE (ADD TOTALS FOR LINES C, D, AND E) | | | | | $1176 |
| G | ASSIGNMENT RECORDING FEE | | | | $40 | $40 |
| | **LIST INDEPENDENT CLAIMS 1, 7, 15, 21, 29 and 31 | | | | | |

_____ Please charge my Deposit Account No. $0 **A copy of this sheet is enclosed.**
_____ the amount of
X A check in the amount of $1176 to cover the filing fee is enclosed.
X A check in the amount of $40 to cover Assignment Recordation fee is enclosed.

X _ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 16.1805. **A copy of this sheet is enclosed.**
_X_ Any filing fees under 37 CFR 1.16 for the presentation of extra claims.
_X_ Any patent application processing fees under 37 CFR 1.17.

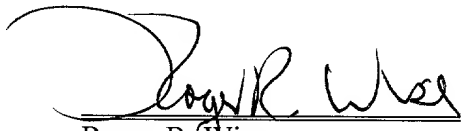
___ The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 16-1805.

___ Any patent application processing fees under 37 CFR 1.17.

___ The issue fee set in 37 CFR 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 CFR 1.311(b).

___ Any filing fees under 37 CFR 1.16 for presentation of extra claims.

Respectfully submitted,



Dated: June 29, 2000

Roger R. Wise
Reg. No. 31,204

PILLSBURY MADISON & SUTRO LLP
725 South Figueroa Street, Suite 1200
Los Angeles, CA 90017-5443
Telephone: (213) 488-7100
Facsimile: (213) 629-1033

PATENT
81674-265754

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|---|---|
| In re application of:<br>Ernie F. Brickell<br>Serial No.: NOT ASSIGNED<br>Filed: June 29, 2000<br>For: SYSTEM AND METHOD FOR CREATION AND USE OF STRONG PASSWORDS | Group No.: NOT ASSIGNED<br><br>Examiner: NOT ASSIGNED |

CERTIFICATE OF MAILING VIA U.S. EXPRESS MAIL
"Express Mail" Mailing Label No. EL 594 170 469 US
Date of Deposit: June 29, 2000

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

I hereby certify that

X Letter of transmittal
X Check in the amount of $1176 as filing fee.
X Patent application (29 pages of specification; 34 claims; 1 pages of abstract)
X 7 sheets of formal drawings
X Declaration
X Executed assignment, with Recordation Cover Letter and check in amount of $40
X Return postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service with sufficient postage under 37 CFR 1.10 on the date indicated above and are addressed to:

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231.

June 29, 2000

Ramon Navarrete

Signature

APPLICATION FOR
UNITED STATES PATENT
IN THE NAME OF

Ernie Brickell

for

# SYSTEM AND METHOD FOR CREATION AND USE OF STRONG PASSWORDS

prepared by:
PILLSBURY MADISON & SUTRO LLP
1100 New York Avenue, N.W.
Ninth Floor, East Tower
Washington, D.C. 20005-7100
(213) 488-7100
Attorney Docket No. 81674-265754
Client Reference No. P8802

Express Mail No.: EL 594 170 469 US

# SYSTEM AND METHOD FOR CREATION AND USE OF STRONG PASSWORDS

## BACKGROUND OF THE INVENTION

1. Field of the Invention:

The present invention relates to computer networks and network security, and in particular, to systems and methods for creating and using strong passwords.

2. Related Art:

Public networks, such as the Internet, hold tremendous potential for many industries. The public networks provide users with vast amount of data that can be quickly and cost effectively accessed from virtually anywhere. The Internet, for example, allows users to access databases such as web page servers from any computer connected to the Internet.

Along with the emergence of public networks and the content/service providers therein comes an imperative need to preserve the confidentiality of some of the sensitive information supplied by the web page servers. If such measure is not taken, sensitive or private information may be accessed, modified, or intercepted by an unauthorized party. Therefore, web page servers must be able to confirm the identity of their online users or visitors before granting access to private information.

A user identification and password combination has long been used as ways to authenticate a user, and public key cryptographic systems are used to provide digital signatures and encryption. A password often comprises a secret series of characters that enables a user to access a file, computer, or program. On multi-user systems, each user must enter his or her password before the computer will respond to

commands. The password essentially helps to determine that a user requesting access to a computer system is really that particular user.

Besides the user identification and password combination, questions and answers combination is also used for authentication and protection purpose. Instead of entering a secret password associated with a user identification, a user is presented with a series of questions and asked to provide answers to the questions. These questions are pre-stored on a remote server, with which the user has previously registered and created the questions and answers corresponding to the questions. Examples of such questions may be inquiries regarding the user's birthday and city of birth. Upon receiving the answers provided by the user, the remote server compares the answers provided by the user with the answers pre-stored on the remote server. If the former answers and the latter answers are the same, the user is granted access to sensitive or private information such as a cryptographic key or private record.

Currently, the market offers implementations of questions and answers to form passwords. However, these questions are released without prior authentication. This allows anyone, including an unauthorized user, to obtain the questions without first being authenticated. The unauthorized person could then do research on the questions to find the answers. Once the unauthorized person obtains the answers to the questions, he/she could use them to impersonate the authorized user and obtain sensitive or private information of the authorized user. For example, one's cryptographic key or private record may be obtained.

Another problem lies in the fact that these present implementations store the actual answers to the questions or the hash of each answer on a remote server that

manages access to restricted information. This further exposes the answers from attack within. Therefore, there is a need for a system and method of providing and using strong passwords while avoiding storing actual answers or the hash of each answer in a remote server.

## BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 shows a network environment in which the present systems and methods may function according to an embodiment of the present invention;

FIG. 2 shows processes for creating a pass phrase according to an embodiment of the present invention;

FIG. 3 illustrates an exemplary use of the pass phrase according to an embodiment of the invention;

FIG. 4 illustrates processes for entering a pass phrase according to an embodiment of the present invention;

FIG. 5 illustrates an exemplary use of the pass phrase to retrieve data protected by the pass phrase according to an embodiment of the invention;

FIG. 6 illustrates in more detail the procedures for requesting a retrieval question in the processes shown in FIG. 4 according to an embodiment of the present invention; and

FIG. 7 illustrates in more detail the procedures for determining whether a retrieval answer is correct in the processes shown in FIG. 4 according to an embodiment of the present invention.

## DETAILED DESCRIPTION

Embodiments of the present invention are directed to a system and method of providing and using strong passwords. FIG. 1 is a diagram illustrating an exemplary computer network in which concepts consistent with the present invention may be implemented. According to an embodiment of the present invention, the computer network includes multiple client workstations 100 coupled to network 110, which may be, for example, the Internet. Each client workstation 100 typically includes a processor 101 operatively coupled to computer memory 102 and a display 103. The processor 101 executes program instructions stored in the computer memory 102, such as client program 105 or viewing program 106.

A user 120 may use any of the client workstations 100 to communicate with a remote server 160 or a content server/relying party 140. In general, the remote server 160 assists the user 120 in creating and providing a strong pass phrase. The content server 140 may be a web site wishing to provide encrypted information to the user 120, or more simply, any party that wishes to rely on the authenticity of information received from the user 120. In an exemplary use, the content server 140 accepts the digital credentials issued from a credential issuing service. Information retrieved from the content server 140 or the remote server 160 is rendered by viewing program 106 and displayed to the user 120 via display 103. The user 120 reads the information being displayed and, if required, enter the requested response as dictated by the information being displayed. The viewing program 106 may be, for example, web browser programs such as Microsoft Internet Explorer, available from Microsoft Corporation, of Redmond, Washington.

The remote server 160 includes a remote server program 165, which interacts with the client program 105 at the client workstation 100 or with a content server program 145 at the content server 140 in implementing a strong pass phrase. The remote server program 165 may, for example, provide a credential service and a retrieval service. In general, the credential service authenticates the identity of the user 120 when the user 120 wishes to retrieve questions stored in the remote server 160. The retrieval service assists the user 120 in setting up questions and answers for constructing a strong pass phrase, storing questions and answers (or hash of the answers), and retrieving questions on an as-needed basis when entering a pass phrase.

The client program 105 allows questions and answers to be obtained and information transmitted to the remote server 160, answers to be combined into a single pass phrase, and specific questions to be chosen for display. In addition, the client program 105 may also include the function of encryption, decryption, authentication, and digitally signing of information being transmitted to and received from the content server 140 or the remote server 160. For example, the client program 105 decrypts information from any one of the servers and provides it to the viewing program 106 for display to the user 120. The client program 105 may also encrypt and/or digitally sign information entered by the user 120 before transmitting it to any one of the servers. Although shown as a separate program from the viewing program 106, the client program 105 and the viewing program 106 may be integrated as a single program, which could also include a credential program that authenticates the identity of a user.

Moreover, although shown as a single program, the client program 105 may be a multitude of programs each providing part of the functionality of the client program 105.

The client workstations 100, by virtue of their connection to the network 110, may send information or may access and retrieve information stored at the content server 140 or the remote server 160. The content server 140 and the remote server 160 may, for example, be implemented by computers or networks of computers. The content server 140 and the remote server 160 accept information requests, such as requests for content or for creating and/or providing a pass phrase, from the client workstation 100 and transmit requested content to the client workstation 100. In addition, they accept and verify digitally signed messages from the client workstation 100. In one exemplary use, the content server 140 interacts with the remote server 160 to register and authenticate a user's credential.

As with the client workstation 100, each of the servers may include at least one processor and computer memory. The memory includes programs that deal with requests from the client workstation 100. These programs interact with the programs on the client workstation 100, such as the client program 105, to carry out desired functions. Additionally, each of the servers may interact with a database (not shown) to respond to information requests from the client workstation 100. The server program may be a web server program such as any one of a number of well-known web servers. For example, the servers may be an Apache web server, a Netscape server (available from Netscape Communications Corporation, of Mountain View, California), or a Microsoft Internet Information Server. Alternatively, the server program may transmit information to the client workstation 100 in a proprietary, non web page format.

The client workstation 100 and the servers may accept program instructions from a computer storage device (e.g., optical or magnetic disk) or from the network 110. Basic input/output system (BIOS) code (i.e., computer instructions) causing the system to implement the disclosed techniques may be programmed into a non-volatile portion of the computer memory 102. The BIOS may be programmed when the system is manufactured or may be later delivered via a computer readable medium.

The client processor 101 and the processors of the server can be any of a number of well-known devices, such as processors from Intel Corporation, of Santa Clara, California. More generally, the client workstation 100 may be any type of computing platform connected to a network which interacts with application programs, such as a personal digital assistant or a "smart" cellular telephone or pager.

In one embodiment, user generated questions and answers are used to produce a pass phrase with high entropy in a way that can be easily remembered by the user 120. To protect against an adversary obtaining the questions and researching the answers, multiple levels of questions and answers are used. There is a single retrieval question and answer, and multiple pass phrase questions and answers. The client program 105 at the client workstation 100 interacts with programs residing at the servers, such as the content server program 145 and/or the remote server program 165, directly or indirectly to perform various functions.

One set of functions relates to creating a pass phrase. These functions include, among other functions, obtaining a plurality of pass phrase questions and pass phrase answers, creating a pass phrase from the plurality of pass phrase answers, obtaining a

set of retrieval questions and retrieval answers, creating a single retrieval pass phrase, and transmitting necessary information to the remote server 160 or content server 140.

Another set of functions relates to providing a pass phrase at a client workstation. These functions include, among other functions, displaying a plurality of entries for entering a plurality of pass phrase answers, creating a single pass phrase from the plurality of pass phrase answers, providing an option for displaying a plurality of pass phrase questions pre-stored in the remote server 160, displaying a plurality of pass phrase questions if the user 120 enters a retrieval answer matching the retrieval answer pre-stored in the remote server 160.

In one exemplary use, the pass phrase is used to wrap cryptographic keys. The cryptographic keys may, for example, be fixed keys or roaming keys. In this example, the remote server 160 stores cryptographic keys that are encrypted with the pass phrase. The client program 105 interacts with programs residing at the servers directly or indirectly to further process the pass phrase, wrap the cryptographic keys using the processed pass phrase, and authenticate the user 120 using the processed pass phrase.

FIG. 2 illustrates processes for creating a pass phrase with high entropy in a way that can be easily recreated by a user 120. In block P200, the user 120 is presented with a display that gives the user 120 examples of how to pick questions that can be easily remembered. In one implementation, the user 120 is asked to create a retrieval question (RQ) and a certain number of pass phrase questions (PPQs). The user 120 is advised to choose an RQ that he/she is likely to remember, so that the user 120 will rarely be required to see it.

In block P210, the user creates the RQ and a retrieval answer (RA) corresponding to the RQ as well as the PPQs and pass phrase answers (PPAs) corresponding to the PPQs. In one implementation, all the answers, RA and PPAs, are covered with asterisks ("*"), so that someone watching the screen will not see the answers. To ensure that the answers are entered correctly, the user is asked to enter all of the answers twice. If, in any particular answer, a first entered answer does not match with the second entered answer, the user is asked to enter that particular answer twice until a first entered answer matches with a second entered answer.

Upon receiving all the answers, the PPAs are used to construct a pass phrase in block P220. In one implementation, an applet combines the PPAs into a single pass phrase. The applet, such as a small Java application, may be downloaded from the content server 140 or the remote server 160 and run on the client workstation 100 by the viewing program 106 equipped with Java virtual machines. The applet concatenate the PPAs together with a fixed random value and apply a cryptographic hash function to the concatenation. One suitable cryptographic hash function is the 160 bit Secure Hash Algorithm (SHA), which is well known in the cryptographic art. The cryptographic hash function may be repeated multiple times in order to increase the difficulty of a brute force attack on the pass phrase. One suitable method for repeating SHA multiple times is with the Public Key Cryptographic Standard (PKCS) #5 algorithm, available from Rivest-Shamir-Adleman (RSA), Inc., of Bedford, Massachusetts. In one exemplary use, the user's pass phrase is converted into a key for encrypting cryptographic keys by using the PKCS #12 algorithm.

In general, hashing algorithms take arbitrary strings as input, and produce an output of fixed size that is dependent on the input. Ideally, it should never be possible to derive the input data given the hash algorithm's output. For a hashing algorithm to be cryptographically secure, such as the SHA algorithm, it must be very difficult to find two input strings that produce the same output hash value, or to find an input string that produces a given hash value.

On the client workstation 100, a local applet constructs a message that consists of the distinguished name (DN) or credential identification, the RQ, the RA, the number of PPQs, the list of PPQs, and the pass phrase, as shown in block P230. In another embodiment, the message may include more, fewer, or different items. For example, the message may include a hash of the RA or a single retrieval pass phrase created from the RA in place of the RA, or the message may not include the number of PPQs. In block P240, this message is signed by the user's private key.

In block P250, the message and signature are routed to a remote server 160 in a secure manner. In one implementation, an applet computes a session key using a cryptography algorithm such as the Diffie-Hellman procedure. The session key encrypts the message and signature, and the encrypted message and signature are sent to the remote server 160. Upon receiving the encrypted message and signature, the remote server 160 decrypts the message.

After the message and signature are received in a secure manner, the remote server 160 determines whether the signature is correct in block P260. If the signature is correct, the remote server 160 will store the RQ, the RA or the hash of the RA, the number of PPQs (if included), the list of PPQs, and the pass phrase, as shown in block

P270. In one embodiment, a data storage key may be implemented to encrypt the above listed data before they are stored, providing an extra level of protection. In another implementation, the remote server 160 returns an acceptance message to the client workstation 100 in the event that the signature is correct. If the signature is incorrect, the remote server 160 returns an error message to the client workstation 100, and the listed data are not stored, as shown in block P275.

FIG. 3 illustrates an exemplary use of the pass phrase according to an embodiment of the invention. In this example, the pass phrase is further processed by the client workstation 100 to wrap data before the data is sent to the remote server 160. In block P300, the pass phrase is hashed in two ways to form an identification key HP1 and an encryption key HP2 at the client work station 100. In one implementation, the HP1 is a public-private key pair, and is used in authenticating the user 120. In one implementation, the client program 105 contains two random numbers. The first random number and the pass phrase are input to a first hashing function, and the second random number and the pass phrase are input to a second hashing function. Based on these inputs, the first and second hashing functions generate HP1 and HP2, respectively.

In block P310, the HP2 is used to wrap the data. In one embodiment, the data is a key token that contains the user's private key and the user's certificate/credential. In another embodiment, HP2 is used only to wrap the user's private key and not the whole key token. In using the HP2 derived from the pass phrase, which in turn derives from the PPAs, the PPAs themselves are actually used to help protect the wrapped data, and not just to protect access to the wrapped data.

In block P320, the HP1 and the key token wrapped by the HP2 are sent securely to the remote server 160. In one implementation, a session key is created and a key exchange protocol is utilized to secure the transmission between the client workstation 100 and the remote server 160. The session key is a symmetric key and is used for securing a single session. At the client workstation 100, the session key encrypts the key token and HP1. Then, the encrypted key token and HP1 are sent to the remote server 160, where they are decrypted.

After the key token and HP1 are received by the remote server 160 in a secure manner, the remote server 160 stores the HP1 and the key token wrapped by the HP2, as shown in block P330. In one implementation, the HP1 and the key token are stored in a table or a database. The table or database may include entries relating to the DN or credential identification of possible users of the remote server 160, the HP1 associated with each of these possible users, and the user's private key wrapped by the HP2 associated with each of the users.

In block P340, the remote server 160 sends an acknowledgement message, which indicates that the HP1 and the key token have been stored, back to the client workstation 100. Upon receiving the acknowledgment message, the client workstation 100 destroys the local copy of the key token.

By storing only the concatenate and hash form of the PPAs in the remote server 160, actual PPAs is not stored on the remote server 160. All the answers to the PPQs are hashed together. By choosing good questions, the entropy can be high enough so that an exhaustive search over all of the answer space is infeasible. Even though the hash of the answers is known to the remote server 160, the actual answers remain

unknown. Thus, an authorized user who breaks into or has access to the remote server 160 cannot simply obtain the PPAs to retrieve the sensitive or private information.

FIG. 4 illustrates processes for entering a pass phrase at a client workstation. From a client workstation 100, a user 120 contacts a content server 140 or a remote server 160. For example, the user may wish to access restricted information from the content server 140 or the remote server 160. In block P400, the user 120 is presented with a screen on the display 103 with k boxes, where k is the number of PPAs that are required, as shown in block P400. In one implementation, this number is determined from the number of the PPQs stored in the remote server 160. The screen on the display 103 also has an option for the user 120 to request the PPQs, in the event that the user 120 does not remember the PPAs of the top of his/her head.

In block P410, it is determined whether the user 120 needs to request PPQs by verifying whether the user 120 chooses to enter the PPAs immediately or chooses the requesting of PPQs option. If the user 120 does not need to request the PPQs and chooses to enter the PPAs immediately, the user 120 enters the PPAs in block P450. On the other hand, if the user 120 needs to request PPQs and chooses the requesting of PPQs option, the user is presented with a screen on the display 103 to enter the RA in block P420.

The screen on the display 103 also offers an option to request the RQ. In block P430, it is determined whether the user 120 needs to request the RQ by verifying whether the user 120 chooses to enter the RA immediately or chooses the requesting of RQ option. If the user 120 does not need to request the RQ and chooses to enter the RA immediately, the user 120 enters the RA in block P440. On the other hand, if the

user 120 needs to request RQ and chooses the requesting of RQ option, procedures for requesting RA, including checking the user's identification information for authorization, are carried out in block P431. These procedures are described in more detail below. Upon receiving the RQ from the remote server 160, the user 120 is presented with a screen that contains the RQ and a box for entering the RA, as shown in block P432. In one implementation, an applet is used to achieve this presentation.

In block P440, the user 120 enters the RA. After the RA is entered, the procedures for requesting the PPQs are carried out. These procedures are described in more detail below. If the RA is correct and the requesting of the PPQs is successful, the user is presented with a screen on display 103 that contains PPQs and boxes for entering the PPAs, as shown in block P442. With the screen prompting the user 120 to enter the PPAs, the user 120 enters the PPAs in block P450. An applet concatenates the PPAs to form a pass phrase and return the pass phrase as the output of this procedure, as shown in block P460.

FIG. 5 illustrates an exemplary use of the pass phrase to retrieve data protected by the pass phrase according to an embodiment of the invention. In this example, the data protected by the pass phrase is illustrated by the user's private key or key token. In other embodiments, other kinds of data may be protected or the pass phrase may simply be used for authentication purpose. In block P500, the pass phrase generated from the PPAs entered by the user 120 is hashed to form HP1 and HP2 using the same hashing functions that were used when creating and registering the pass phrase (e.g., FIG. 3). In block P510, HP1 is sent to the remote server 160 for authentication. In block 520, the remote server 160 receives the HP1 and determines if authentication is

successful by comparing the HP1 received with the HP1 pre-stored in a table or database. In one implementation, the remote server 160 authenticates the user by matching the transmitted HP1 to the corresponding value in the table or database.

If the received HP1 is different from the pre-stored HP1, indicating that the PPAs entered are incorrect, an error message is sent to the user 120, as shown in block P525. In one implementation, the user is asked to enter the PPAs again, with the option to request the PPQs if needed. On the other hand, if the authentication is successful, the user's wrapped key token or user's key token with wrapped private key is sent back to the user 120 at the client workstation 100, as shown in block P530.

In block P540, upon receiving the wrapped key token, the client workstation 100 uses HP2 as the key to unwrap the key token through a decryption algorithm. The algorithm is the same algorithm used to wrap the private key initially, such as the Data Encryption Standard algorithm. This allows the user 120 to recover the data. In this example, roaming credential and the private key are recovered. With the private key and credential/certificate in hand, the user 120 can utilize the secure communication channel. Having the digital credential, the content server 140 can now obtain the credential management facility's authentication of the user's credentials.

FIG. 6 illustrates in more detail the procedures for requesting a RQ according to an embodiment of the present invention. After the client workstation 100 determines that the user needs to request RQ before proceeding, a local applet forms a request for RQ message, the message containing identification information, as shown in block P600. In one implementation, the identification information may be the DN or credential identification. The identification information is used to check the identity of the user 120

to make sure that the user 120 is an authorized user. In block P610, a local applet creates a session key using a cryptography algorithm such as the Diffie-Hellman procedure. The applet encrypts the request for RQ message using the session key and sends it to the remote server 160, as shown in block P620.

Upon receiving the request for RQ message, the remote server 160 decrypts the message and determines if the identification information indicates an authorized user, as shown in block P630. In one implementation, the remote server 160 will check the DN or credential identification contained in the request for RQ message against the DN or credential pre-stored in the remote server 160. For example, the pre-stored DN or credential may be obtained when the user registered with the remote server 160 and may be stored in a table or database contained in the remote server 160. If the identification information is not valid, as shown in block P635, an error message is returned to the user and the user is asked to send another request for the RQ using different identification information.

If the identification information is valid, the remote server 160 returns the RQ associated with the user 120, the RQ being encrypted with the session key, as shown in block P640. Like all transactions, this event will be recorded in an event log of the credential. In one implementation, the remote server 160 returns the RQ based on the identification information received, which is mapped to an RQ in a table or database pre-stored in the remote server 160. Upon receiving the encrypted RQ, the client workstation 100 decrypts the RQ using the session key, allowing the RQ to be displayed on the display 103.

All communication between the user and the server can be encrypted using a similar or some other method.

FIG. 7 illustrates in more detail the procedures for determining if the RA entered by the user 120 is correct and requesting PPQs, according to an embodiment of the present invention. After the user 120 enters the RA, a local applet forms a request for PPQs message, the message containing identification information and the RA, as shown in block P700. In one implementation, the identification information may be the DN or credential identification. In block P710, a local applet creates a session key using a cryptography algorithm such as the Diffie-Hellman procedure. The applet encrypts the request for PPQs message and sends it to the remote server 160, as shown in block P720.

Upon receiving the request for PPQs message, the remote server 160 decrypts the message and determines if the identification information indicates an authorized user and if the RA is correct, as shown in block P730. In one implementation, the remote server 160 will check the DN or credential identification contained in the request for RQ message against the DN or credential pre-stored in the remote server 160.

If the identification information or the RA is not valid, as shown in block P735, an error message is returned to the user. Depending on the situation, the user 120 may be asked to send another request for the PPQs using different identification information, or the user may be asked to enter another RA, or both. In one embodiment, if the user 120 fails consecutively to enter the correct RA or the identification information, the remote server 160 begins to increase the delay time between allowed credential attempts for the user 120.

If the identification information and the RA are valid, the remote server 160 returns the PPQs associated with the user 120, the PPQs being encrypted with the session key, as shown in block P740. Like all transactions, this event will be recorded in an event log of the credential. In one implementation, the remote server 160 returns the PPQs based on the identification information, which is mapped to a set of PPQs in a table or database pre-stored in the remote server 160. Upon receiving the encrypted PPQs, the client workstation 100 decrypts the PPQs using the session key, allowing the PPQs to be displayed on the display 103.

According to an embodiment of the invention, the system and method described above further provides the feature of notifying the user 120 when anyone asks for the user's RQ. Such notification may be accomplished through various communication means. For example, an e-mail, an instant message, a page, or a facsimile may be sent to the user 120. The user 120 is provided with the feature to immediately change the user's RQ if the person who requested the RQ is not the user 120. The person, without knowledge of the RA to the new RQ, will not be able to obtain the PPQs. In one implementation, if a user is bothered by someone who constantly asks for the user's RQ, the user could put in a null question.

While the description above refers to particular embodiments of the present invention, it will be understood that many modifications may be made without departing from the spirit thereof. The accompanying claims are intended to cover such modifications as would fall within the true scope and spirit of the present invention. The presently disclosed embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the

appended claims, rather than the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

**CLAIMS**

What is claimed is:

1. A method of creating a strong pass phrase, the method comprising:

obtaining a plurality of questions and a plurality of answers corresponding to the plurality of questions; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

2. The method of claim 1, further comprising transmitting the plurality of questions to a remote server.

3. The method of claim 2, further comprising:

obtaining a set of retrieval questions and a set of retrieval answers corresponding to the set of retrieval questions;

combining the set of retrieval answers into a single retrieval pass phrase; and

transmitting the set of retrieval questions and the retrieval pass phrase to the remote server.

4. The method of claim 3, wherein the plurality of questions consists of a plurality of pass phrase questions, the plurality of answers consists of a plurality of pass phrase answers corresponding to the pass phrase questions, the set of retrieval questions consists of a retrieval question, and the set of retrieval answers consists of a retrieval answer corresponding to the retrieval question.

5. The method of claim 1, wherein the plurality of questions are obtained by displaying a plurality of partial questions and obtaining completions to said plurality of partial questions.

6. The method of claim 1, wherein the pass phrase is used to wrap data to be stored in a remote server.

7. A method of providing a pass phrase at a client workstation, the method comprising:

displaying a plurality of entries for entering a plurality of pass phrase answers; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

8. The method of claim 7, further comprising displaying the plurality of pass phrase questions corresponding to a plurality of pass phrase answers pre-stored in a remote server.

9. The method of claim 8, further comprising obtaining the plurality of pass phrase questions from the remote server.

10. The method of claim 9, further comprising providing an option for displaying the plurality of pass phrase questions.

11. The method of claim 10, further comprising requiring a retrieval pass phrase before the remote server will release the plurality of pass phrase questions, wherein the retrieval pass phrase is pre-stored in the remote server and is formed from a set of retrieval answers previously entered by a user.

12. The method of claim 11, further comprising providing an option for displaying a set of retrieval questions which corresponds to the set of retrieval answers and pre-stored in the remote server.

13. The method of claim 12, wherein a user having registered the set of retrieval questions is notified if anyone asks for the set of retrieval questions.

14. The method of claim 12, further comprising displaying the set of retrieval questions.

15. A computer readable medium for use in conjunction with a client workstation and a server for creating a strong pass phrase, the computer readable medium including computer readable instructions encoded thereon for:

obtaining a plurality of questions and a plurality of answers corresponding to the plurality of questions; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

16. The computer readable medium of claim 15, further including computer readable instructions encoded thereon for comprising transmitting the plurality of questions to a remote server.

17. The computer readable medium of claim 16, further including computer readable instructions encoded thereon for:

obtaining a set of retrieval questions and a set of retrieval answers corresponding to the set of retrieval questions;

combining the set of retrieval answers into a single retrieval pass phrase; and

transmitting the set of retrieval questions and the retrieval pass phrase to the remote server.

18. The computer readable medium of claim 17, wherein the plurality of questions consists of a plurality of pass phrase questions, the plurality of answers consists of a plurality of pass phrase answers corresponding to the pass phrase questions, the set of retrieval questions consists of a retrieval question, and the set of retrieval answers consists of a retrieval answer corresponding to the retrieval question.

19. The computer readable medium of claim 15, wherein the plurality of questions are obtained by displaying a plurality of partial questions and obtaining completions to said plurality of partial questions.

20. The computer readable medium of claim 15, wherein the pass phrase is used to wrap data to be stored in a remote server.

21. A computer readable medium for use in conjunction with a client workstation for providing a pass phrase at a client workstation, the computer readable medium including computer readable instructions encoded thereon for:

displaying a plurality of entries for entering a plurality of pass phrase answers; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

22. The computer readable medium of claim 21, further including computer readable instructions encoded thereon for displaying the plurality of pass phrase questions corresponding to a plurality of pass phrase answers pre-stored in a remote server.

23. The computer readable medium of claim 22, further including computer readable instructions encoded thereon for obtaining the plurality of pass phrase questions from the remote server.

24. The computer readable medium of claim 23, further including computer readable instructions encoded thereon for providing an option for displaying the plurality of pass phrase questions.

25. The computer readable medium of claim 24, further including computer readable instructions encoded thereon for requiring a retrieval pass phrase before the remote server will release the plurality of pass phrase questions, wherein the retrieval pass phrase is pre-stored in the remote server and is formed from a set of retrieval answers previously entered by a user.

26. The computer readable medium of claim 25, further including computer readable instructions encoded thereon for providing an option for displaying a set of retrieval questions corresponds to the set of retrieval answers and pre-stored in the remote server.

27. The computer readable medium of claim 26, wherein a user having registered the set of retrieval questions is notified if anyone asks for the set of retrieval questions.

28. The computer readable medium of claim 26, further including computer readable instructions encoded thereon for displaying the set of retrieval questions.

29. A client workstation comprising:

a processor;

a display connected to the processor;

a computer memory connected to the processor, the computer memory including:

a viewing program for rendering information received from a server on the display, the display displaying a plurality of entries for entering a plurality of pass phrase answers and an option for requesting a plurality of pass phrase questions corresponding to the plurality of the pass phrase of answers, and

a client program for combining the pass phrase answers to form a single pass phrase,

wherein if the option for requesting the set of the pass phrase questions is chosen, an entry for entering a retrieval answer and an option for requesting a retrieval question corresponding to the retrieval answer is displayed.

30. The client workstation of claim 29, wherein if the option for requesting the retrieval question is chosen, a request is formed and transmitted to the server, which authenticates the request and returns the retrieval question for display if authentication is successful, and if the retrieval answer is entered immediately or entered after the retrieval question is displayed, the validity of the retrieval answer is determined, and if the retrieval answer is determined to be valid, the pass phrase questions are displayed.

31. A computer network comprising:

a client workstation, the client workstation constructing a pass phrase from a plurality of pass phrase answers entered by a user at the client workstation;

a network connected to the client workstation; and

a server connected to the client workstation through the network, the server receiving a request from the client workstation for a plurality of pass phrase questions corresponding to a plurality of pass phrase answers pre-stored in the server, and in response to the request for pass phrase questions, transmitting a request to the client workstation for a retrieval answer corresponding to a retrieval question pre-stored in the server.

32. The computer network of claim 31, wherein the client workstation transmits a request to the server for the retrieval question if the retrieval answer is not entered immediately by the user, the server authenticates the requests and returns the retrieval question to the client workstations for display if authentication is successful.

33. The computer network of claim 21, wherein if the retrieval answer is entered immediately or entered after the retrieval question is displayed, the validity of the retrieval answer is determined, and if the retrieval answer is determined to be valid, the pass phrase questions are displayed.

34. The computer network of claim 31, further comprising a middle server, through which the client workstation and the server transmit requests and requested information to and from each other.

## ABSTRACT

A system and method is provided for creating and using strong passwords with high entropy. The system and method uses user generated questions and answers. To protect against an adversary from obtaining the questions and researching the answers, multiple levels of questions and answers are used. There are a first set of question(s) and a first set of answer(s) corresponding to the first set of questions as well as a second set of plurality of questions and a second set of plurality of answers corresponding to the second set of plurality of questions. The second set of plurality of answers is concatenated to form a single pass phrase. To enter the pass phrase at a client workstation, a user is presented with a plurality of entries for entering the second set of plurality of answers and an option to request a second set of plurality of questions. If the option to request a second set of questions is chosen, entry for entering a first set of answer(s) and an option for requesting a first set of question(s) are presented. If the option for requesting the first set of question(s) is chosen, the remote server returns the first set of question(s) after authentication. If the correct first set of answer(s) is entered immediately or entered after the first set of question(s) is displayed, the second set of plurality of questions is displayed.

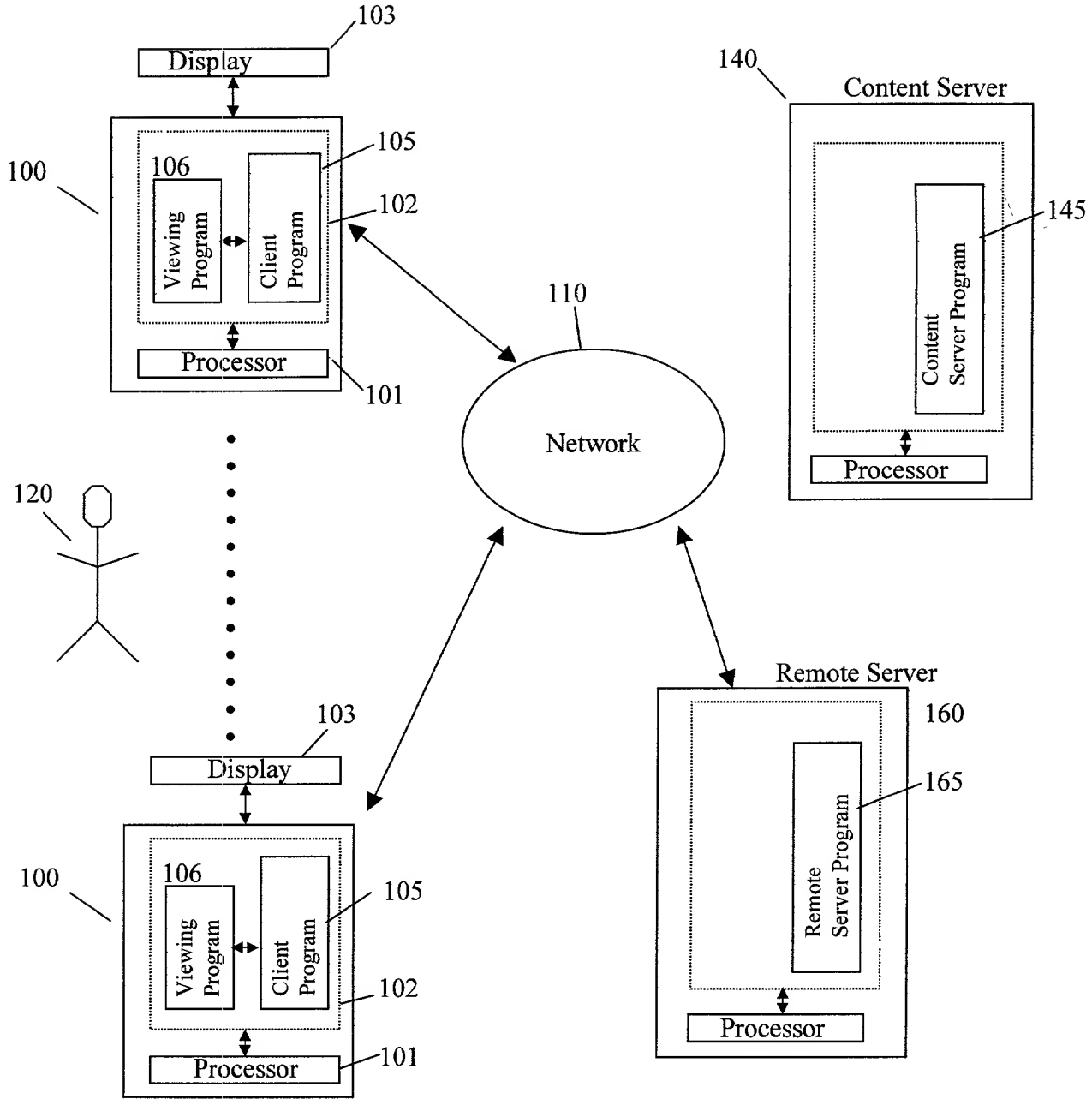

103
Display
140
Content Server
105
106
100
102
145
Viewing Program
Client Program
Content Server Program
110
Processor
101
Network
Processor
120
Remote Server
160
103
165
Display
Remote Server Program
100
106
105
Viewing Program
Client Program
102
Processor
101
Processor

**Fig. 1**

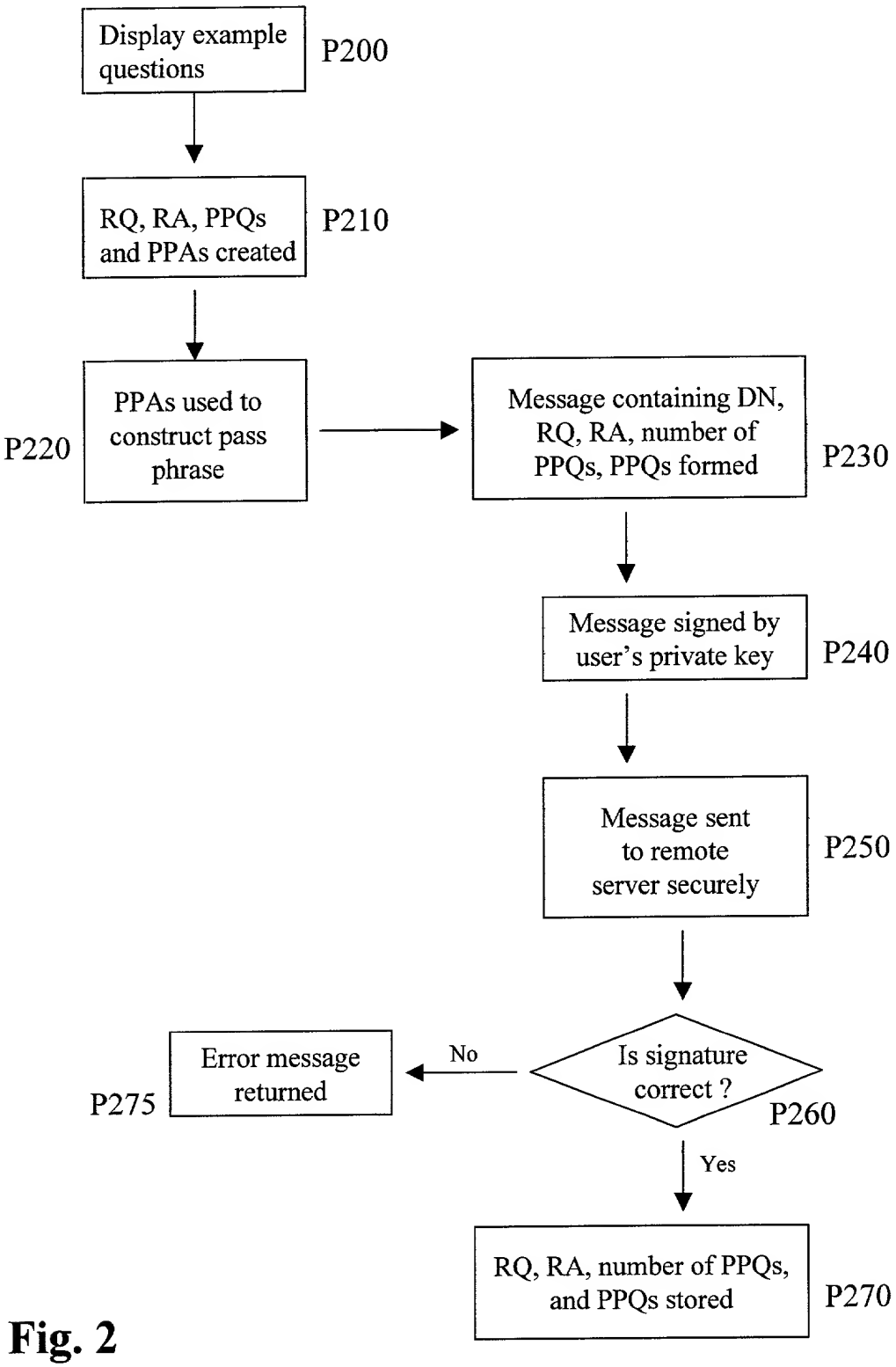

Display example questions
P200
RQ, RA, PPQs and PPAs created
P210
PPAs used to construct pass phrase
P220
Message containing DN, RQ, RA, number of PPQs, PPQs formed
P230
Message signed by user's private key
P240
Message sent to remote server securely
P250
Is signature correct ?
P260
No
Error message returned
P275
Yes
RQ, RA, number of PPQs, and PPQs stored
P270

**Fig. 2**

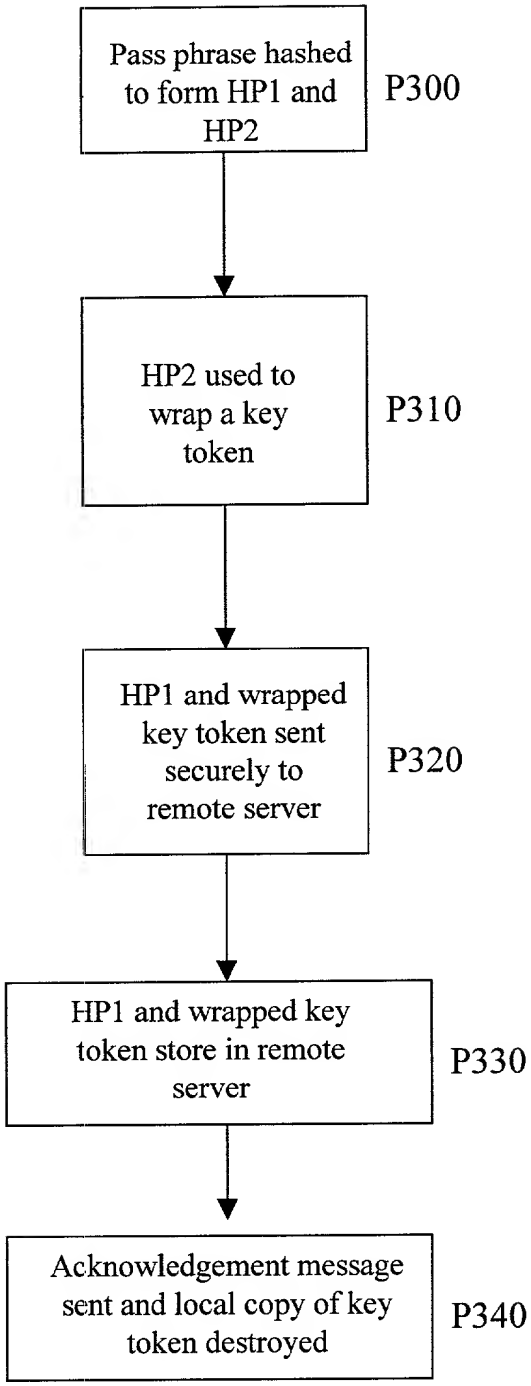

Pass phrase hashed to form HP1 and HP2
P300
HP2 used to wrap a key token
P310
HP1 and wrapped key token sent securely to remote server
P320
HP1 and wrapped key token store in remote server
P330
Acknowledgement message sent and local copy of key token destroyed
P340

**Fig. 3**

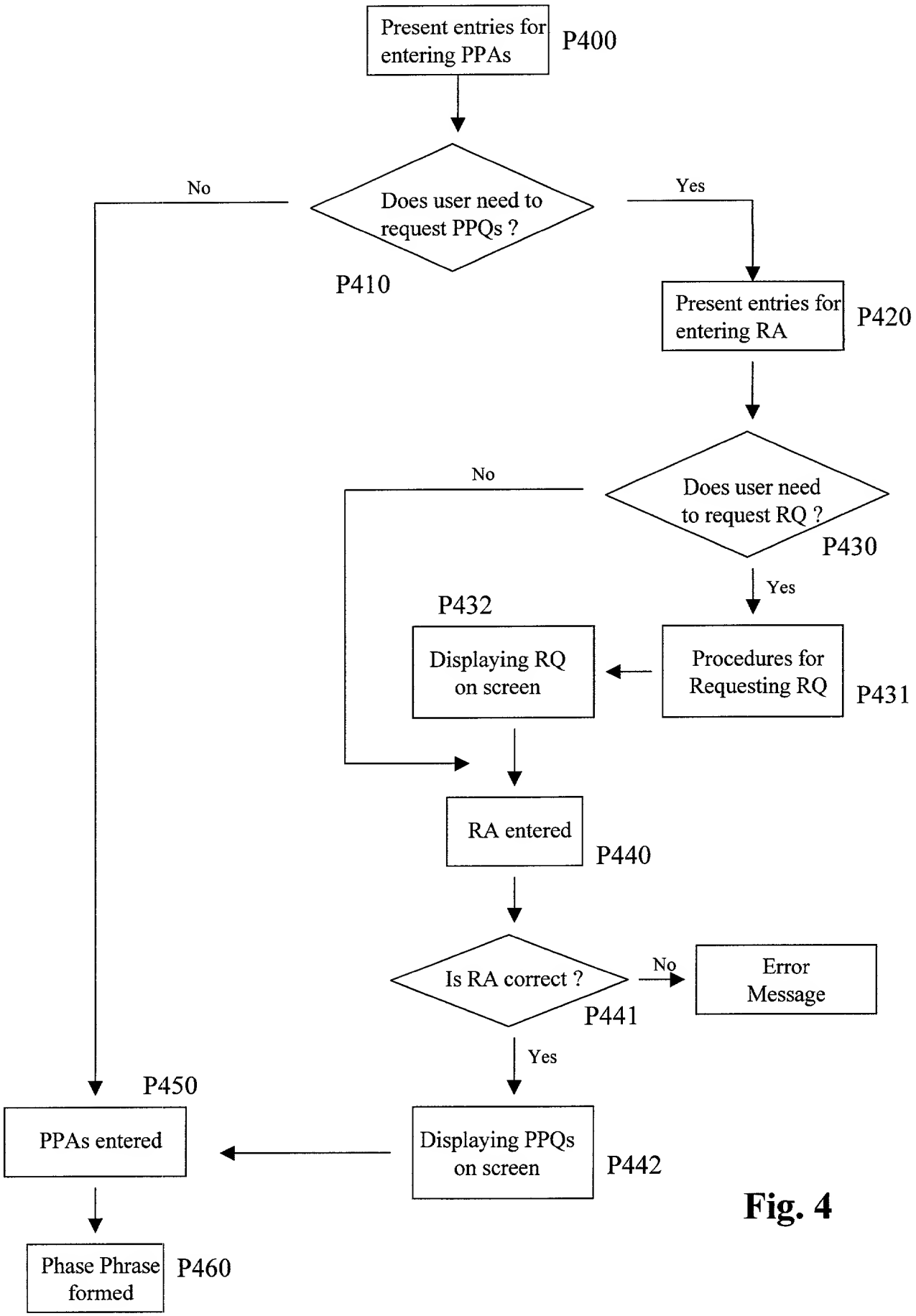

Present entries for entering PPAs
P400
Does user need to request PPQs ?
P410
No
Yes
Present entries for entering RA
P420
Does user need to request RQ ?
P430
No
Yes
P432
Displaying RQ on screen
Procedures for Requesting RQ
P431
RA entered
P440
Is RA correct ?
P441
No
Error Message
Yes
P450
PPAs entered
Displaying PPQs on screen
P442
Phase Phrase formed
P460

Fig. 4

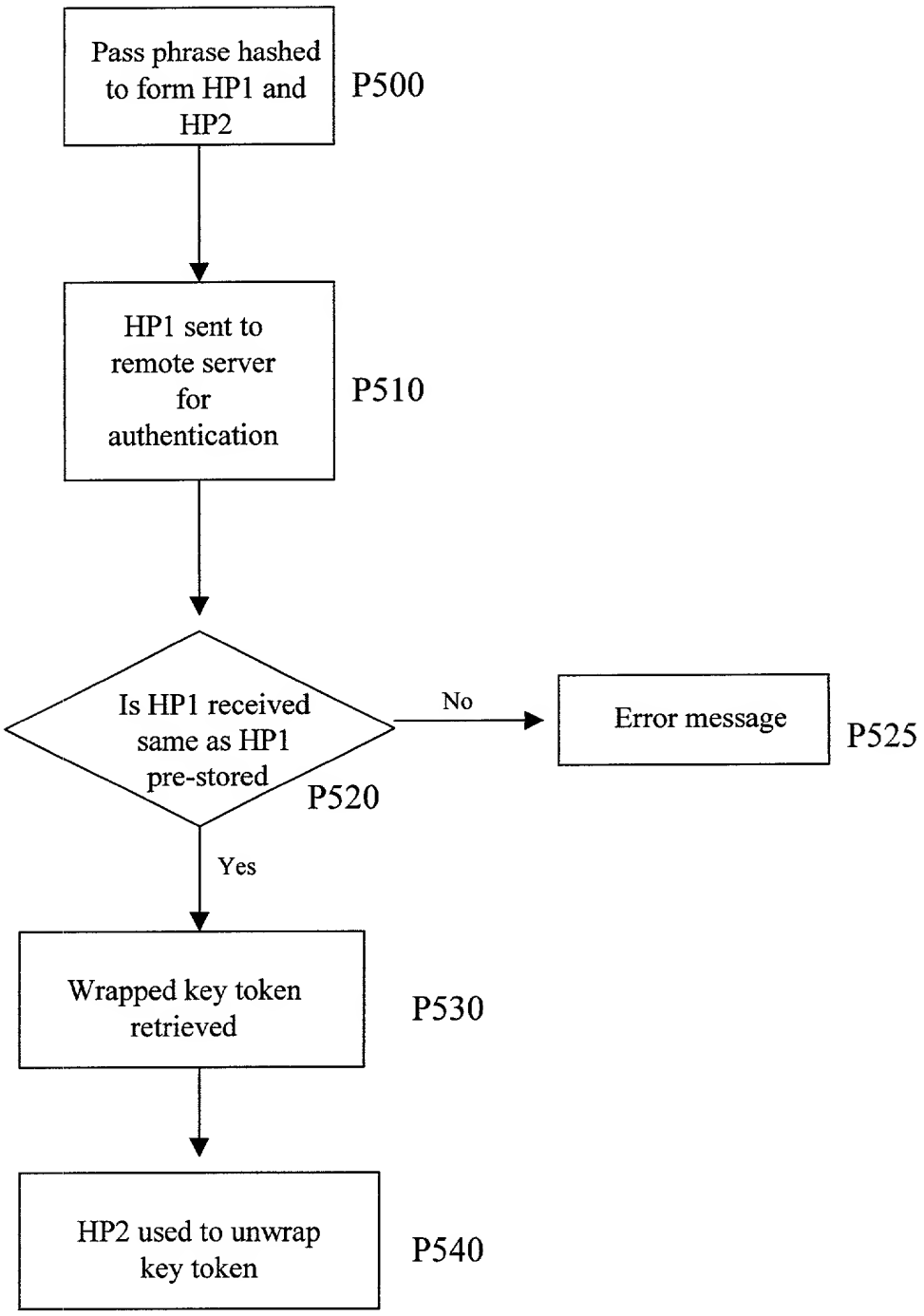

Pass phrase hashed to form HP1 and HP2
P500
HP1 sent to remote server for authentication
P510
Is HP1 received same as HP1 pre-stored
P520
No
Error message
P525
Yes
Wrapped key token retrieved
P530
HP2 used to unwrap key token
P540

**Fig. 5**

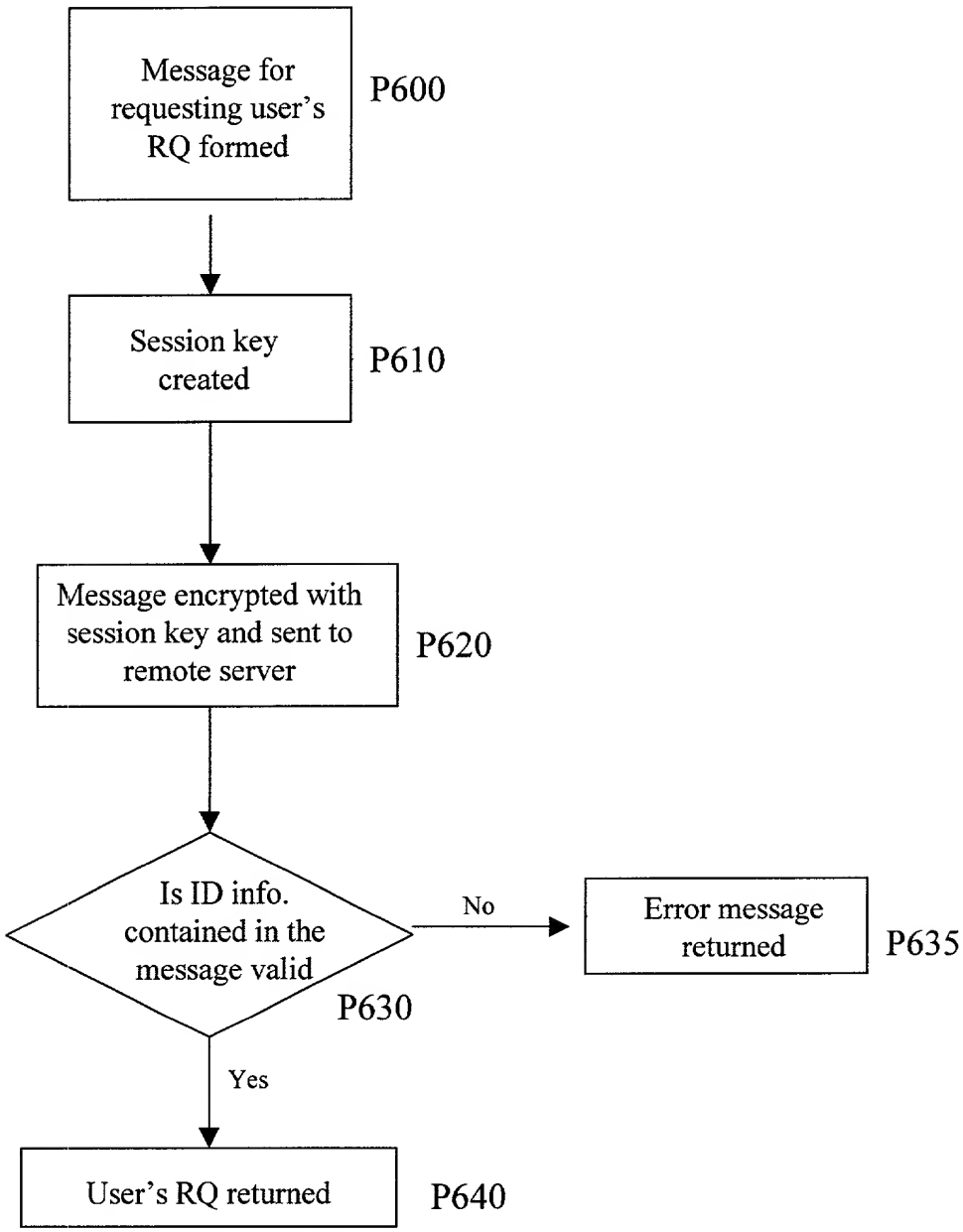

Message for requesting user's RQ formed
P600
Session key created
P610
Message encrypted with session key and sent to remote server
P620
Is ID info. contained in the message valid
P630
No
Error message returned
P635
Yes
User's RQ returned
P640

**Fig. 6**

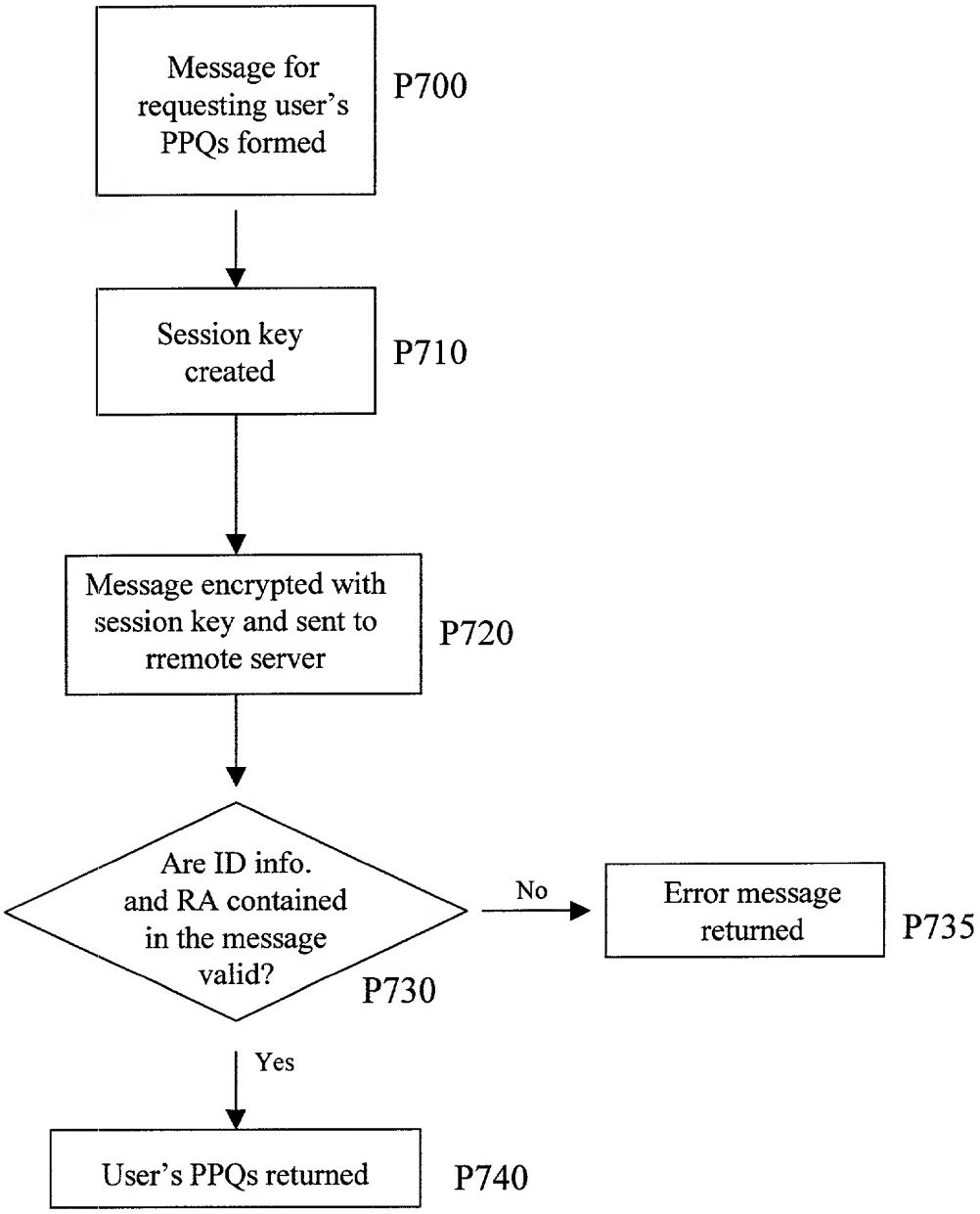

Message for requesting user's PPQs formed
P700
Session key created
P710
Message encrypted with session key and sent to rremote server
P720
Are ID info. and RA contained in the message valid?
P730
No
Error message returned
P735
Yes
User's PPQs returned
P740

**Fig. 7**

FOR UTILITY/DESIGN
CIP/PCT NATIONAL/PLANT
ORIGINAL/SUBSTITUTE/SUPPLEMENTAL
DECLARATIONS

# RULE 63 (37 C.F.R. 1.63) DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PM & S FORM

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name, and I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the **INVENTION ENTITLED: SYSTEM AND METHOD FOR CREATION AND USE OF STRONG PASSWORDS**

the specification of which (CHECK applicable BOX(ES) )

X A. ☒ is attached hereto.

BOX(ES) → B. ☐ was filed on _____ as U.S. Application No. ____/_____

→ → C. ☐ was filed as PCT International Application No. PCT/ ____/_____ on _____

and (if applicable to U.S. or PCT application) was amended on _____

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose all information known to me to be material to patentability as defined in 37 C.F.R. 1.56. Except as noted below, I hereby claim foreign priority benefits under 35 U S.C 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT International Application which designated at least one other country than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International Application, filed by me or my assignee disclosing the subject matter claimed in this application and having a filing date (1) before that of the application on which priority is claimed, or (2) if no priority claimed, before the filing date of this application:

| PRIOR FOREIGN APPLICATION(S) Number | Country | Day/MONTH/Year Filed | Date first Laid-open or Published | Date Patented or Granted | Priority NOT Claimed |
|---|---|---|---|---|---|
| | | | | | |

**If more prior foreign applications, X box *at bottom* and continue on attached page.**

Except as noted below, I hereby claim domestic priority benefit under 35 U S C. 119(e) or 120 and/or 365(c) of the indicated United States applications listed below and PCT international applications listed above or below and, if this is a continuation-in-part (CIP ) application, insofar as the subject matter disclosed and claimed in this application is in addition to that disclosed in such prior applications, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in 37 C.F.R. 1.56 which became available between the filing date of each such prior application and the national or PCT international filing date of this application:

| PRIOR U.S. PROVISIONAL, NONPROVISIONAL AND/OR PCT APPLICATION(S) Application No. (series code/serial no.) | Day/MONTH/Year Filed | Status pending, abandoned, patented | Priority NOT Claimed |
|---|---|---|---|
| 60/ [P8802; 81674-265754] | April 21, 2000 | pending | |

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

And I hereby appoint Pillsbury Madison & Sutro LLP, Intellectual Property Group, 1100 New York Avenue, N.W., Ninth Floor, East Tower, Washington, D C 20005-3918, telephone number (202) 861-3000 (to whom all communications are to be directed), and the below-named persons (of the same address) individually and collectively my attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith and with the resulting patent, and I hereby authorize them to delete names/numbers below of persons no longer with their firm and to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/ organization who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct the above Firm and/or a below attorney in writing to the contrary.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Paul N. Kokulis | 16773 | Dale S. Lazar | 28872 | Mark G. Paulson | 30793 | W. Patrick Bengtsson | 32456 |
| Raymond F. Lippitt | 17519 | Paul E. White, Jr. | 32011 | Stephen C. Glazier | 31361 | Jack S. Barufka | 37087 |
| G. Lloyd Knight | 17698 | Glenn J. Perry | 28458 | Paul F. McQuade | 31542 | Adam R. Hess | 41835 |
| Carl G. Love | 18781 | Kendrew H. Colton | 30368 | Ruth N. Morduch | 31044 | William P. Atkins | 38821 |
| Kevin E. Joyce | 20508 | G. Paul Edgell | 24238 | Richard H. Zaitlen | 27248 | Paul L. Sharer | 36004 |
| George M. Sirilla | 18221 | Lynn E. Eccleston | 35861 | Roger R. Wise | 31204 | James R. Thein | 31710 |
| Donald J. Bird | 25323 | Timothy J. Klima | 34852 | Jay M. Finkelstein | 21082 | Peter Lam | 44855 |
| Peter W. Gowdey | 25872 | David A. Jakopin | 32995 | Michael R. Dzwonczyk | 36787 | Gene I. Su | 45140 |
| Alan K. Aldous | 31905 | Robert D. Anderson | 33826 | Joseph R. Bond | 36458 | Richard C. Calderwood | 35468 |
| Jeffrey S. Draeger | 41000 | Cynthia Thomas Faatz | 39973 | Sean Fitzgerald | 32027 | Seth Z. Kalson | 40670 |
| David J. Kaplan | 41105 | Charles A. Mirho | 41199 | Leo V. Novakoski | 37198 | Naomi Obinato | 39320 |
| Thomas C. Reynolds | 32488 | Kenneth M. Seddon | 43105 | Mark Seeley | 32299 | Steven C. Skabrat | 36279 |
| Howard A. Skaist | 36008 | Steven C. Stewart | 33555 | Raymond J. Werner | 34752 | Robert G. Winkle | 37474 |
| Charles K. Young | 39435 | Thomas Raleigh Lane | 42781 | Calvin E. Wells | 43256 | Paul G. Nagy | 37896 |
| Steven W. Smyrski | 38312 | Eric S. Chen | 43542 | Vivian S. Shin | 43919 | | |

| (1) INVENTOR'S SIGNATURE: | Ernie Brickell | | F. | BRICKELL | Date: 6/28/00 |
|---|---|---|---|---|---|
| | First | | Middle Initial | Family Name | |
| Residence | Portland | | Oregon | | USA |
| | City | | State/Foreign Country | | Country of Citizenship |
| Post Office Address | 3106 N.W. Luray Terrace, Portland, Oregon | | | | |
| (include Zip Code) | ~~87111~~ 97210 | | | | |

| (2) INVENTOR'S SIGNATURE: | | | | | Date: |
|---|---|---|---|---|---|
| | | | | | |
| | First | | Middle Initial | Family Name | |
| Residence | | | | | |
| | City | | State/Foreign Country | | Country of Citizenship |
| Post Office Address | | | | | |
| (include Zip Code) | | | | | |

FOR ADDITIONAL INVENTORS, "X" box ☐ and proceed on the attached page to list each additional inventor.

☐ See additional foreign priorities on attached page (incorporated herein by reference).

Atty. Dkt. No. PM81674-265754

**Rule 56(a) & (b) = 37 C.F.R. 1.56(a) & (b)**
**PATENT AND TRADEMARK CASES - RULES OF PRACTICE**
**DUTY OF DISCLOSURE**

(a) ...Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the [Patent and Trademark] Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability...(b) information is material to patentability when it is not cumulative and (1) It also establishes by itself, or in combination with other information, a prima facie case of unpatentability of a claim or (2) refutes, or is inconsistent with, a position the applicant takes in: (i) Opposing an argument of unpatentability relied on by the Office, or (ii) Asserting an argument of patentability

## PATENT LAWS 35 U.S.C.

### §102. Conditions for patentability; novelty and loss of right to patent

A person shall be entitled to a patent unless--

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent or

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States, or

(c) he has abandoned the invention, or

(d) the invention was first patented or caused to be patented, or was the subject of an inventor's certificate, by the applicant or his legal representatives or assigns in a foreign country prior to the date of the application for patent in this country on an application for patent or inventor's certificate filed more than twelve months* before the filing of the application in the United States, or

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent, or

(f) he did not himself invent the subject matter sought to be patented, or

(g) before the applicant's invention thereof the invention was made in this country by another who had not abandoned, suppressed, or concealed it. In determining priority of invention there shall be considered not only the respective dates of conception and reduction to practice of the invention, but also the reasonable diligence of one who was first to conceive and last to reduce to practice, from a time prior to conception by the other.

### §103. Condition for patentability; non-obvious subject matter

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made. . . .

(c) Subject matter developed by another person, which qualified as prior art only under subsection (f) or (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

* Six months for Design Applications (35 U.S.C. 172).